DIGITAL TURKISH LIRA

First Phase Evaluation Report

2023

TÜRKİYE CUMHURİYET
MERKEZ BANKASI

TÜRKİYE CUMHURİYET
MERKEZ BANKASI

CONTENTS

Definitions and Abbreviations

1 Introduction

2 Central Bank Digital Currency Requirements, Principles and Approaches

3 Digital Turkish Lira Design

4 Findings and Assessments

5 Following Phases

6 Conclusion

APPENDIX

DEFINITIONS AND ABBREVIATIONS

TABLE 1 - DEFINITIONS

Asymmetric Encryption	A method of encryption in which the key that encrypts the information and the key that decrypts it are different
Digital Identity	Information that digitally represent persons, organizations, assets, or things
Distributed Ledger Technology	A general name given to distributed database and application technologies that can be operated with many independent nodes and participants, with trust boundaries between participants
Financial Inclusion	A measure of the extent to which financial products and services are made available to individuals or businesses
Financial Intermediary Institution	Authorized institution that intermediates natural or legal persons' access to financial products and services
Issuance	The process of generating money and verifiable credentials in the Digital Turkish Lira System
Key Exchange	Sharing of own public keys by parties who want encrypted communication over an insecure medium
Near Field Communication	A communication protocol that enables short-range and wireless data transfer between electronic devices
Node	One of the network stakeholders that collectively run the distributed ledger with responsibilities such as storing ledger data, confirming transactions, or providing communication according to the operating principles of the distributed ledger network
Operator	An institution or institutions in charge of operating the digital currency system
Permissioned Distributed Ledger	Distributed ledger platforms where only participants authorized by specific authorities can take on specialized responsibilities such as approving and recording transactions
Permissionless Distributed Ledger	Distributed ledger platforms where all participants that meet the requirements of the specified protocols can join the network and assume specialized responsibilities such as approving and recording transactions
Phase-1	First phase of the Central Bank Digital Turkish Lira Research and Development Project
Phase-2	Second phase of the Central Bank Digital Turkish Lira Research and Development Project
Phase-3	Third phase of the Central Bank Digital Turkish Lira Research and Development Project
Platform	Digital Turkish Lira Collaboration Platform
Private Key	The key used in asymmetric encryption algorithms, access to which must be restricted to the generator of the key or authorized party
Project	Central Bank Digital Turkish Lira Research and Development Project
Proof-of-Concept	Implementation and execution in a test environment to investigate and demonstrate the feasibility of a new concept, idea, or method
Public Key	Publicly accessible key used in asymmetric encryption algorithms
QR Code	Two-dimensional code with black and white modules in the form of square black-and-white dots or pixels that store alphanumeric data, characters, and symbols
Redemption	Withdrawal of money from circulation in the Digital Turkish Lira System
Smart Contract	Snippets of code that automatically fulfill the requirements of a contract when conditions are met
User	Natural or legal person that receives service in the Digital Turkish Lira System
World Wide Web Consortium	The organization that sets standards for the World Wide Web

DEFINITIONS AND ABBREVIATIONS

TABLE 2 - ABBREVIATIONS

ATM	Automated Teller Machine
BIS	Bank for International Settlements
CBRT	Central Bank of the Republic of Türkiye
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
EFT	Electronic Fund Transfer System
ESTS	Electronic Securities Transfer System
FAST	Instant and Continuous Transfer of Funds System
FSB	Financial Stability Board
G20	Group of 20
IBAN	International Bank Account Number
NFC	Near-Field Communication
R&D	Research and Development
SSI	Self-Sovereign Identity
TPS	Transactions Per Second
UTXO	Unspent Transaction Output
VC	Verifiable Credential
VP	Verifiable Presentation
W3C	World Wide Web Consortium

1. Introduction

1. Introduction

The Central Bank of the Republic of Türkiye (CBRT) continues its work on the feasibility of introducing a digital Turkish lira complementary to the existing payments infrastructure. With the Central Bank Digital Turkish Lira Research and Development (R&D) Project, the CBRT aims to determine the potential features of the digital Turkish lira, test different architectural setups and technological alternatives, and conduct pilot tests.

The CBRT's research and development work for the Central Bank Digital Currency first started **in 2020 with proof-of-concept studies.** Following the successful completion of the proof-of-concept study, which included tests of the applicability of various distributed ledger technologies to the Central Bank Digital Currency, the Central Bank Digital Turkish Lira Research and Development Project was launched. Under the responsibility of the **Digital Currency R&D team** established within the Central Bank, the research, development and testing of the project are being carried out in addition to the proof-of-concept studies in related fields.

The CBRT has a well-established technical capacity for developing and operating its own Real Time Gross Settlement payment systems. However, to build an operating capacity for digital currency including cryptography, specialized hardware and various advanced technologies, which are considered essential but do not fall within the expertise of a central bank, the CBRT decided to collaborate with leading technology stakeholders. Accordingly, **in 2021,** the CBRT signed bilateral memorandums of understanding with TÜBİTAK, the Scientific and Technological Research Council of Türkiye, and technology companies ASELSAN and HAVELSAN. The **"Digital Turkish Lira Collaboration Platform" (Platform)** was established with the participation of these technology stakeholders. Technological research, development and testing processes were carried out in close cooperation with the stakeholders during the first phase of the project.

2020

● Digital Currency R&D studies launched

2021

● Digital Currency proof-of-concept completed

● Technology partners identified and the Collaboration Platform established

2022

● Phase-1 launched

● First pilot test conducted

2023

● Phase-1 completed

2024

○ Phase-2

While wholesale and retail payments[1] are mainly differentiated depending on the audience to which they are given access, retail payments formed the framework for the first phase. As part of the first phase, the work on setting up the required environments started **in 2022** and **the first payment transactions on the Digital Turkish Lira System were executed successfully** in the pilot tests carried out at the end of the same year. In the first half of 2023, pilot tests continued, leading to the **completion of the first phase.** In line with the findings, it is planned to move on to advanced phases where more widespread pilot tests will be carried out. Additionally, **the Digital Turkish Lira Collaboration Platform will be expanded with the involvement of new participants** based on the analyzes and evaluations to be made after completing the project phases.

[1] While users in wholesale payments are institutions, users in retail payments are citizens. Due to this distinction in users, wholesale payments involve transactions in large amounts but low in volume, while retail payments involve transactions in small amounts but high in volume.

The CBRT carries on its work to prepare for all aspects of the circulation of the digital Turkish lira. In subsequent periods, priority will be given to studies on the **economic and legal framework** of the digital Turkish lira, as well as its technological requirements, and the results of these studies will be presented **to decisionmakers.** Once the final decision is made and the relevant legislation is implemented, it will be possible for the CBRT to accelerate its work on expanding the use of the digital Turkish lira, making it available throughout Türkiye.

In the first phase, which is the subject of this Evaluation Report, the "Phase-1 Digital Turkish Lira System" was developed with the Platform participants, pilot tests were conducted and preliminary tests of strategic technologies were carried out. In the pilot test studies during this phase, the aim was to conduct tests at specific locations and to **measure the user experience and system performance** through these tests.

The scope of the first phase consisted of:

- Preparation of the technical working environment where the Digital Turkish Lira System tests will be carried out
- Preparation of the infrastructure for the Digital Turkish Lira System tests
- Establishment of a distributed ledger platform for the Digital Turkish Lira System
- Design and development of smart contracts and applications to be run with the distributed ledger platform
- Integration of a prototype digital identity system with the Digital Turkish Lira System
- Design and development of a digital wallet application for digital Turkish lira transactions
- Simulation and testing of issuance, distribution, online payment/transfer and redemption scenarios of the digital Turkish lira
- Cyber security operations
- Conduct of pilot test processes, and
- Measurement of system performance and user experience.

The Evaluation Report serves to share the findings of the R&D studies conducted at the CBRT and the first phase conducted with Platform stakeholders, as well as the approaches adopted in the project.

In the second phase, the Digital Turkish Lira Collaboration Platform will be expanded with the involvement of new participants, and pilot tests of different scenarios will be conducted.

1.1 What is Central Bank Digital Currency?

> ***Digital Turkish lira is the* digital form of the Turkish lira*. Its unit is the Turkish lira as in the current form of fiat money.***

Banknotes, introduced directly for public use by central banks, are produced from various physical materials such as cotton, linen, paper and polymers. Conventional banknotes, put into circulation in physical form on demand, are unable to serve in digital economic activities in their current form and are losing their function as a medium of exchange in such digital environments. Therefore, for digital payments, banknotes need to be transformed into payment instruments with digital equivalents, such as bank deposits, or additional solutions need to be brought in via cards.

Central banks are conducting research and development projects to make their currencies available in the digital environments with enhanced functionality. The entire process of digitalization of wholesale and retail payments represents different phases of these efforts. Digitalization will be able to offer an alternative architecture in payments without the wholesale-retail distinction. In the simplest terms, Central Bank Digital Currency, which can be regarded as the final stage of the digitalization of payments, can be defined as the **digital form of a sovereign country's currency.**

While a Central Bank Digital Currency (hereinafter referred to as digital currency) may bring to mind crypto assets, it is important to note that a **digital currency is not a crypto asset.** In economic terms, digital money is the digital form of the banknote used as the national currency.[2] Digital currency is a new form of **national currency which is the single national unit for measuring value,** is defined as a legal means of payment, and represents social consensus by taking its power from national sovereignty. It is therefore critical to recognize that digital currency and crypto assets are completely different concepts in terms of both economic and legal frameworks. In this respect, the digital Turkish lira refers to the **digital form of the Turkish lira.** Its unit is the Turkish lira, as in the current form of fiat money.

[2] Debates and considerations are multi-dimensional, unique, and new for each country. This report is neither intended to end legal and economic debate, nor to adopt or dictate an absolute terminology on the issue.

The CBRT was among the first institutions to conduct studies on electronic money. It began such work in 1998, and has been pioneering economic digitalization for years with its theoretical studies, as well as practical implementations and breakthroughs such as EFT, Electronic Securities Transfer System (ESTS) and FAST. From an economic perspective, deposits and electronic money, as currently defined,[3] differ from money and hence from digital money as they solely serve as means of payment. However, all the work in this regard directly facilitates the digitalization of money, and payments in particular.

The digital Turkish lira will be designed and developed in such a way that it has the capacity to create opportunities out of new technological potentials as well as economic activities, which have been digitalized in an increasingly rapid fashion due to the pandemic. Emerging technologies will enhance the functionality of money, but the nature of money will remain the same. Accordingly, designs are developed in view of the main features of money.

Financial inclusion

Complementary payment channel

Uniformity in digital payments

Programmable payments

Once circulated, the digital Turkish lira is expected to make various contributions such as **enhanced financial inclusion, development of a complementary payment channel** in line with the principle of uninterrupted and continuous operation of payments,[4] **uniformity in digital payments,** and **a base for innovative uses upon the development of a programmable payments infrastructure.** These benefits will be elaborated on in the following sections.

[3] Money issued and electronically stored by electronic money institutions against a fund.

[4] https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/The+Role+of+Central+Banks+in+the+Payment+Systems/

1.2 Opportunities of Digital Currency

The CBRT initiated its digital currency studies with a view to seek an effective solution in the context of financial dynamics in Türkiye and in response to relevant global developments. As a matter of fact, the research and studies on digital currency around the world are carried out in line with countries' own strategic goals. These efforts are not independent of each country's political, geographical and socioeconomic conditions. Certain countries that have progressed in digital currency efforts prioritize it as a solution to improve their banking infrastructure and increase financial inclusion. While the targets of reducing cash usage and digitalization also steer a number of countries' digital currency initiatives, other motivations include factors such as dominance in payment systems and strategic autonomy, depending on country dynamics. In addition to these ongoing efforts on digital currencies for retail payments, various proof-of-concept and pilot studies are being conducted on digital currencies intended for wholesale payments, exclusively available to financial institutions. Moreover, as part of the goal of "increasing the efficiency of cross-border payments," which was set forth at the G20 meetings in 2020, the BIS, commissioned by the FSB, has been carrying out various projects targeting cross-border transfer of digital money at its offices and innovation hubs.

The CBRT observes that the internet, which stands out with its functionality in generating, distributing, reproducing and interpreting data and information, has evolved into a new type of value-sharing environment. In this new setting, assets and identities are digitalized while the protection of personal data is also considered. Accordingly, the CBRT assesses that the circulation of digital currency may lay the groundwork for the following opportunities in the medium and long term:

Financial Technologies Ecosystem

Financial Technologies Center

Continuous and Instant Financial Data

Smart Payments

Offline Payments

Disaster-Resilient Digital Payments

A More Functional Form of Money

Sovereign Digitalization Capacity

Financial Technologies Ecosystem: The CBRT considers digital currency an important component of the rapidly developing financial technology ecosystem in Türkiye. The aim is to make the digital Turkish lira a key building block for the growth of financial technologies ecosystem in the country by integrating it with both existing and new financial technology platforms. Efficiency gains in the financial services sector are also expected to add to potential growth.

Financial Technologies Center: Worldwide examples reveal that the use of many new generation financial technologies is yet to mature. It is believed that these technologies, which will enter daily life in a more developed form and in a more efficient way with digital currency, may provide opportunities in global markets. Digitalization of money seems to be one of the tools that will provide a relative advantage in the competition to become a global financial technology hub.

Continuous and Instant Financial Data: To increase efficiency in decision-making processes, data-driven approaches combined with personal data protection measures are gaining prominence. In this context, both cryptology, and artificial intelligence and machine learning-based solutions are expected to contribute to data analysis. The use of the digital form of money will enable the generation of new financial data as well as the emergence of additional data sources and recording environments. New data and advanced data analytics methods will contribute to decision-making processes. Additionally, different and innovative workflows will emerge on the back of implementations in which various data are user-managed, and users will be able to benefit from their own data in a more secure and efficient way. Besides, as assets and “things” will be identified, digital currency will contribute to the execution of automatic accounting processes.

Smart Payments: The digitalization of money will bring about concepts and innovations in everyday life, such as conditional controls on money[5] or on the transfer of money within payment systems, streaming payments, the economy of things and invisible payments. These innovations will improve the efficiency and user experience of payment flows. The more effective and practical the processes required for economic activities can be made, the easier it will be to remove obstacles to continuous innovation. In an ideal digitalized payments ecosystem, thanks to smart payments, it will be possible to meet all the needs of economic units in a fully comprehensive, secure and privacy-preserving manner, without unnecessary delays and at minimal cost.

Offline Payments: Digital currency is intended to offer an offline and contactless digital payment alternative that complements cash. Although offline payments have been a priority for a number of countries and institutions for years, no product has yet been developed that fully meets all needs and is currently operational. The CBRT sees significant opportunities in this regard and considers offline digital payments a service that should be readily available on demand like cash. As well as increasing transaction capacity, offline payments will help achieve uniformity compared to methods that have failed to spread across the country, are fragmented and require different payment instruments at different points.

[5] The CBRT’s choices are given under the Current Approach and Findings and Assessments headings.

Disaster-Resilient Digital Payments: The Digital Turkish Lira Project targets digital payments that ensure uninterrupted access to money and payments in the event of any disaster. The CBRT is designing different ways of using digital currency, both online and offline. Accordingly, it is anticipated that such payment systems will facilitate the uninterrupted circulation of money in the wake of potential disasters.

A More Functional Form of Money: The primary factor that makes a national and sovereign currency strong is its functionality. Goods and services that can be obtained in exchange for the currency are a component of such functionality. The change in the form of money, its transformation into software, which is a more complex form, and the digitalization of offline payments may lead to fundamental functional differences among digital currencies around the world in terms of design, implementation and integration. Making the digital form of the currency more functional relative to its global equivalents is an important way to strengthen the national currency.

Sovereign Digitalization Capacity: Economic activities are inevitably becoming digitalized. The collective digitalization of the global scale of production, distribution and consumption will bring about new standards. In this context, by building a sovereign digitalization capacity, the digital Turkish lira also offers a capacity to contribute to standardization and create a global opportunity for the country.

Serving as a base for the potential gains outlined above, digital currency will be able to strengthen and increase its own functionality with other systems that will be built around it and with which it can be integrated. The identification of all economic units, processes and all kinds of assets in digital environments and the automation of inter-institutional data reconciliation environments will set an example of increasing functionality. To this end, the requirements of digital currency should be defined correctly, the principles in R&D processes should be determined by experience and data-driven decisions, and approaches should be supported by appropriate processes.

2. Central Bank Digital Currency Requirements, Principles and Approaches

2. Central Bank Digital Currency Requirements, Principles and Approaches

Requirements and principles set the basis of approaches in digital currency projects. The key requirements outlined by many central banks for these projects tend to overlap with each other. However, design principles and their implementations may differ.

The requirements and principles set by the CBRT for designs and development of digital currency, and the various approaches adopted and implemented in the current phase, are becoming more evident in light of the experience in R&D processes. It is imperative to meet the key requirements to ensure the uninterrupted and continuous operation of the systems in the event that the digital Turkish lira is circulated as a national currency. Principles are followed in all phases of the Digital Turkish Lira Project, in view of the requirements. Approaches, on the other hand, refer to the designs and methods adopted at the current stage of the work, building upon established principles.

2.1 Key Requirements

Transaction Capacity

Technical capacity should be provided to handle daily money traffic instantaneously.

User Experience

End user should be able to use the system safely and with ease.

Scalability

The system should be able to fulfill requests at times of high traffic, without its performance being impaired.

Security

The system should be highly resistant to internal and external attacks.

Resilience and Availability

The system must be resilient to failures and continuously accessible.

Convertibility

The system should allow for continuous convertibility between digital and other forms of the Turkish lira.

Regulatory Compliance

National and international legislation must be followed.

2.2 Design Principles

Privacy

Users' digital privacy must be protected and data privacy in financial transactions should be ensured to the maximum level. Personal information should only be shared with the parties determined by legal frameworks and to the necessary extent.

Technological and Architectural Flexibility

The system should be able to be designed and organized to adapt to future technological innovations, different architectural preferences and possible new workflows.

Interoperability

The system should be designed to work in harmony with both existing and potential future components of digital ecosystems.

First, Do No Harm

The system should not harm economic and financial processes. It should not aim to compete with existing financial products and services.

Financial Intermediary Independence

The user should be able to register in the system through any licensed financial intermediary, and registered users should be able to access the system through a different licensed financial intermediary with the credentials they have.

2.3 Current Approach

Two-Tier Distribution Model

The digital Turkish lira will be accessed through financial intermediaries, including commercial banks. Banks and licensed participants will be in charge of the distribution of the digital Turkish lira.

Account Independence

Digital Turkish lira accounts will not require a bank account. The accounts will not be dependent on operator infrastructure. Account identifiers will not require financial intermediary information.

One Account Per User

There will be a single and specific account for each user. It will be accessible through all intermediary institutions.

Self-Sovereign Identities

Credentials[6] containing user information will be stored under the control of the user. Verification flows will be processed over a common network. A user will be able to manage a large number of credentials. An identification that links user information to verifiable credentials will be possible.

Hybrid Systems

Conventional and new technologies will be used together.

[6] 6. Detailed information about credentials is given in the Digital Identity System section.

Programmable Payments

The digital money will enable smart payments on a separate layer of programmability. The concept of *programmable payments* is preferred over *programmable money*. In the programmability layer, contract templates can be created, containing the conditions related to credentials and payment interfaces. Contracts can be combined and presented for different use cases. Public institutions and different licensed actors will be able to take part in the development, approval, deployment, presentation, updating and deactivation of contracts.

3. Digital Turkish Lira Design

3. Digital Turkish Lira Design

> ***Digital identity and digital currency systems served as the core systems of Phase-1. Distributed Ledger Technology was used in Phase-1 to better assess the opportunities offered by new technologies.***

In the design of the Digital Turkish Lira System, modularity and the replaceability of technologies in all components are essential. In particular, the abstraction layer and service layer designs allow different alternatives of digital identity and digital currency systems to be tested and integrated. **What is important for the Digital Turkish Lira System is to prepare a system that fully meets the requirements and principles of digital currency rather than the technology itself.** Accordingly, distributed ledger, centralized ledger and hybrid solutions are being tested.

Within the scope of Phase-1, the digital identity system, digital currency system, abstraction layer, service layer and wallet application were identified as the fundamental components, and were prepared and tested using open-source software according to R&D principles. In addition to the main components, there were also components such as security, administration, monitoring, simulation and data analysis. The components sometimes required preparation and development specific to pilot tests. However, the focus was primarily on the use cases of basic components and designs, and on their setups for the following phases.

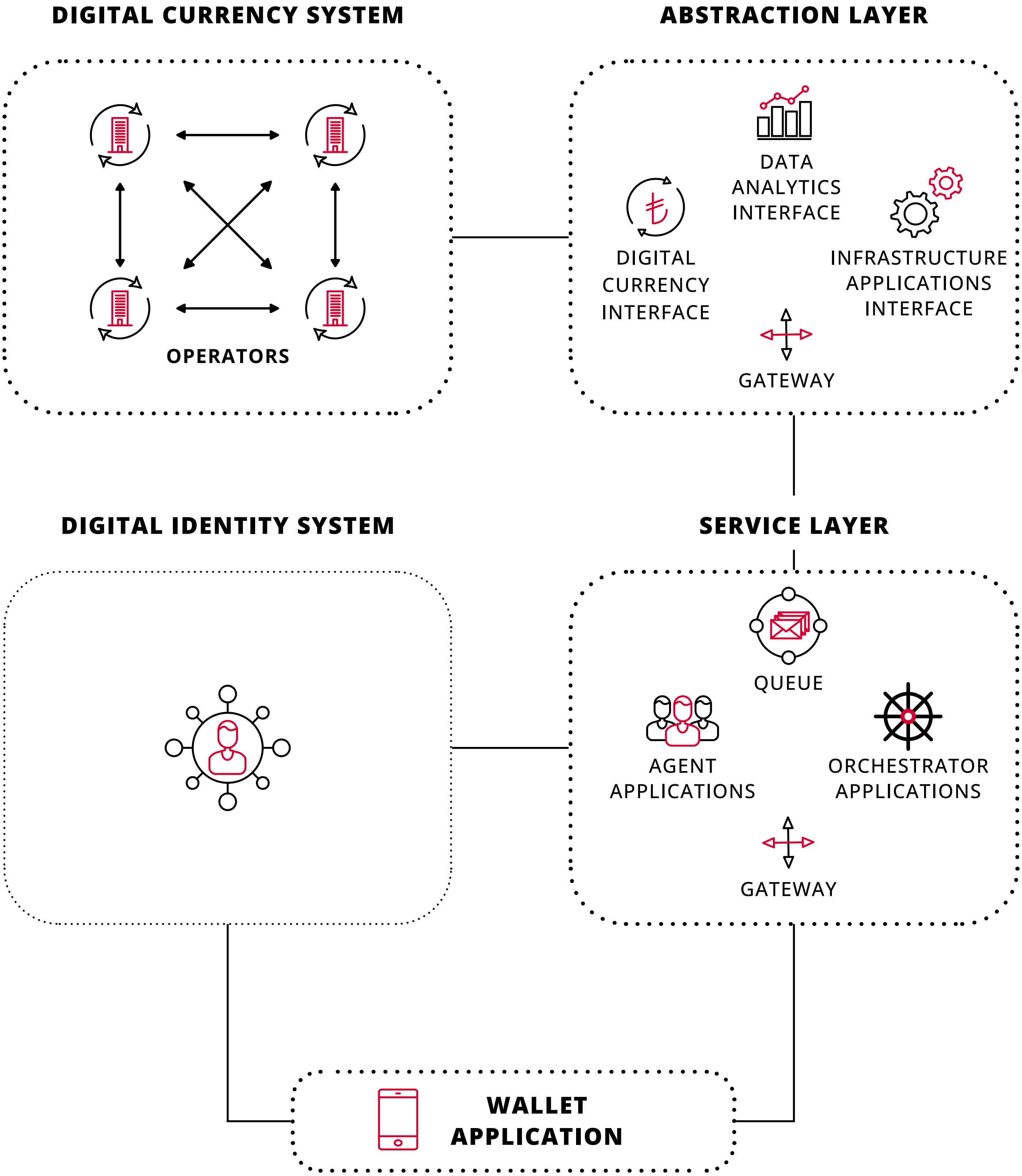
The work undertaken prior to the project suggested that the direct utilization of the current system architectures used in crypto assets in developing digital currency was not technologically and financially feasible. In permissionless distributed ledgers, resource-intensive Sybil attack prevention mechanisms are used to prevent nodes from dominating the network and launching attacks. In permissioned distributed ledgers, participants can be actors with known identities subject to regulation. In this respect, due to the preference for the operator nodes in the digital currency system to be licensed entities, a permissioned distributed ledger network was chosen instead of a permissionless distributed ledger network. However, the CBRT concluded that **certain technologies used in crypto asset networks can be extremely useful in digital ecosystems.** These technologies make technical and practical contributions to the designs in the areas of ensuring privacy, enhancing the availability of payment systems, reducing the dependency on payment intermediaries, and creating smart workflows, particularly programmable payments.

Digital identity and digital currency systems served as the core systems of Phase-1 studies. While it is possible to consider the use of conventional technologies in the design of core systems, the CBRT decided to use Distributed Ledger Technology (DLT) in Phase-1 to better assess the opportunities offered by new technologies and to investigate the compatibility of such technologies with digital currency requirements and principles.

The **abstraction and service layers** were logical partitions that identify the way financial intermediaries[7] participate in the system. As they are regarded as spaces for potential innovation and act as a part of the end-to-end (from mobile device to ledger) use of digital currency, they are considered among the fundamental components. In Phase-1, abstraction and service layers were designed with a distributed and modular approach in mind.

The **wallet application** is the main component that enables users to access the systems and carry out financial transactions. In Phase-1, the digital wallet was implemented as a mobile application. In the following phases, hardware wallets may also be introduced. The aim is to use hardware that meets the requirements to ensure that user data and documents can be securely stored and used in financial transactions.

[7] Operators also assumed the role of financial intermediary in the work carried out in Phase-1.


DIGITAL CURRENCY SYSTEM
OPERATORS
ABSTRACTION LAYER
DATA ANALYTICS INTERFACE
DIGITAL CURRENCY INTERFACE
INFRASTRUCTURE APPLICATIONS INTERFACE
GATEWAY
DIGITAL IDENTITY SYSTEM
SERVICE LAYER
QUEUE
AGENT APPLICATIONS
ORCHESTRATOR APPLICATIONS
GATEWAY
WALLET APPLICATION

3.1 Digital Identity System

In transactions using banknotes, the parties are physically present in the same environment. Therefore, if needed, identity verification can be performed face-to-face, during the payment process. However, since digital payments do not require the parties to be physically present in the same environment, they technically necessitate a digital mechanism to verify identity. Today, one of the most common methods to meet this requirement is digital identity.

While digital identities are widely used, there is still no consensus on a single model. As a result, the preferred models take quite different approaches. In the Digital Turkish Lira Project, a new and decentralized digital identity model, the Self-Sovereign Identity (SSI), was tested. The digital identity system, one of the core systems in the Digital Turkish Lira Project, uses a permissioned distributed ledger designed for the SSI model.[8] Transaction flows in Phase-1 studies were carried out in compliance with the model defined by the W3C.[9] Participants and users in the digital currency system can assume one or more of the roles of credential issuer, holder or verifier.

Verifiable Credentials and Verifiable Presentations

In the SSI model, users keep control of their personal information by storing it in their own wallets. Personal information is stored in **Verifiable Credentials (VC).**

A VC is a document that shows personal information or one or more properties of a person. Driving licenses, diplomas, passports and IDs are examples of documents that can be issued as a credential. In this context, it is even possible to create VCs that are not directly descriptive of the person, but rather indicate an attribute, skill, authority, claim or even past actions of the person. VCs are tamper-resistant, cryptographically authenticated digital credentials.

[8] 8. Detailed information about digital identity models is given in the appendix.

[9] 9. https://www.w3.org/TR/vc-data-model/

A VC may include the following elements:

- Information related to identifying the subject of the VC (e.g. a photo, name, or identification number)
- Information related to the issuing authority (e.g. a university or a public institution)
- Information related to the type of the VC (e.g. a passport, a driving license, or an employee ID)
- Information related to specific attributes or properties being asserted by the issuing authority about the VC subject (e.g. nationality, the classes of vehicle entitled to drive, or date of birth)
- Proof for the validity and integrity of the credential
- Information related to constraints on the VC (e.g. terms of use, or expiration date)

In various use cases, the user may choose to share some, rather than all, of the information in their VC. In other scenarios, the user may share partially selected information from their multiple VCs at once. By signing their VC or VCs, the credential holder generates a **Verifiable Presentation (VP),** and shares it with the credential verifier to prove their claims. The VP enables sharing **only the necessary information** in each transaction. Both the VC and the VP can be transmitted quickly, making them more practical than physical documents for long-distance verification. Moreover, thanks to technologies such as digital signatures, the VC is more resilient to tampering, making it more difficult to forge than physical documents.

Decentralized Identifier

In the SSI model, a **Decentralized Identifier (DID)** is used to identify natural and legal persons. Each user has a unique DID value. The DID value is an identifier consisting of alphanumeric characters.

Under Phase-1, each participant, including end users and financial intermediaries, has a DID value. Like an account number, the DID value can be used for financial transactions with both natural and legal persons. However, unlike account numbers such as IBAN, the DID value **does not contain information on the operator or financial intermediary.** Another difference is that the DID value does not have to be used only in financial transactions. Since the DID can also be used as an identifier in systems other than financial systems, it can be thought of as an identification number similar to the Turkish Identification Number. However, in addition to identifying citizens, the DID value can also be used to identify legal persons, assets and things. Depending on design preferences, DIDs can be generated in a way that makes it indistinguishable whether they belong to a person or a thing based on the DID value.

In the SSI method, participants are able to **share their credentials only to the extent they deem appropriate and only with the people they want,** using the DID they generate and the VCs they store in their own wallet applications.

3.2 Digital Currency System

The digital currency system is the component where transactions are finalized and recorded. Under Phase-1, the digital currency system was envisioned as a **retail payment system,** with each participant having a separate account.

Phase-1 experiments were conducted to observe whether the DLT satisfies the requirements and principles that the digital currency system is expected to meet.

Accordingly, the reasons for choosing the DLT can be summarized as follows:

- Improved system accessibility
- Distributed operational processes and responsibilities
- Technological flexibility
- Enhanced information security and reliability
- Opportunity for innovative payment flows with the help of smart contracts

In Phase-1, a permissioned distributed ledger was used. In both Phase-1 studies and the proof-of-concept studies conducted before Phase-1, comparisons were made among permissioned distributed ledger platforms frequently used in central banks' digital currency projects. While many of these platforms were blockchain,[10] non-blockchain distributed ledger platforms were also tested. It was observed that some platforms were unable to provide the necessary functionality for users to access the system without operator dependency, or suffered severe performance degradation when the number of operators in the network was increased. Modularity and the ability to create a variety of distributed ledger network designs were the differentiating features that shaped platform preferences.

[10] There are different DLT implementations depending on data storage and consensus methods. Blockchain is one of them, but not all DLTs are blockchain.

Account Numbers

The account numbers of personal and corporate users are derived from the DID values created by the users themselves in the wallet application and used when onboarding users with the relevant intermediary. With this account identifier mechanism, users' personal information is isolated from the digital currency system and privacy is strengthened. The users are neither dependent on the financial intermediaries they are registered with nor on the operators that operate nodes in the system, and transactions can be initiated through any operator. In this way, access problems that users may encounter in case an intermediary or operator fails to provide service can be prevented.

Two-Tier Structure

In the digital currency distribution model, the central bank is on the first tier and financial intermediaries are on the second tier. Financial intermediaries can be banks or licensed institutions that comply with the specified regulations. End users participate in the system through financial intermediaries. In the model, the central bank is responsible for the issuance of money and financial intermediaries are responsible for its distribution.

Architecture

The architecture preferred in a digital currency system resembles the "Hybrid Digital Currency"[11] architecture. There may be variants of the hybrid architecture. As a point of divergence, in the digital currency system, **the central bank does not know which account belongs to which user since it does not have the identity information of the end users.** Another point is that financial intermediaries also have accounts in the digital currency system. Since the identity information of intermediary institutions is shared with the central bank, the balances of intermediary institutions can be known by the central bank.

The digital currency system is designed in accordance with the principle of "first, do no harm." In the two-tier structure, which is also used in existing retail payment systems, the central bank does not have a direct relationship with end users, so the operational responsibility for users lies with the second-tier participants. Likewise, the preferred digital currency architecture also allows for a separation of responsibilities compared to a structure where the central bank directly and solely opens an account for

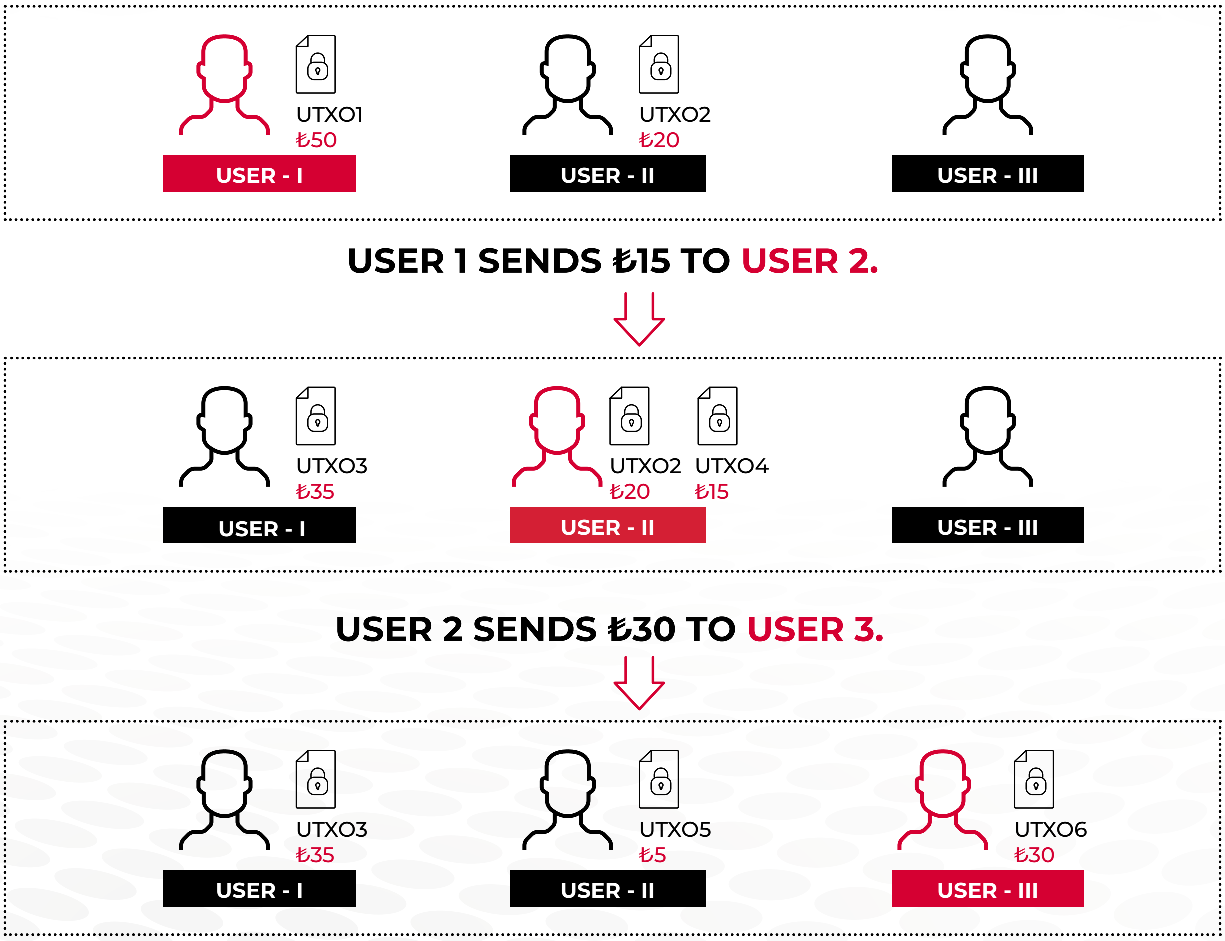
[11] https://www.bis.org/publ/work948.pdf

the end user. In addition, know-your-customer processes can also be carried out by financial intermediaries in line with existing flows of financial service production.

HOW TO STORE DIGITAL CURRENCY INFORMATION?

There is more than one way to record digital currency transactions and express the state of money. The **Unspent Transaction Output (UTXO) model** and the **account (balance) model** are two different methods that can be used in a distributed ledger network.

In the UTXO model, each transaction consists of one or more inputs and one or more outputs. When a new transaction is created, the inputs are spent by referencing the outputs of previous transactions in the user's possession, upon the necessary cryptographic checks. The transaction results in new, unspent outputs that can be referenced as inputs by their holders in future transactions. This model is similar to **the way physical money works.** It can be thought of as changing the ownership of the banknote used in payment, and the total balance of the person is the sum of the banknotes they own.



USER 1 SENDS ₺15 TO USER 2.

USER 2 SENDS ₺30 TO USER 3.

In the account model, the user has a balance associated with their account, and transactions take place in such a way that the balance of the counterparty increases by the amount by which the user's balance decreases. Transactions in the account model are rather similar to transfers between **bank accounts.**

3.3 Abstraction Layer

The main reason for using the Abstraction Layer in the Digital Turkish Lira Project is to increase the modularity of the system. The aim is to ensure that all system parts used in Phase-1 studies operate independently from each other as much as possible, thus minimizing the cost of replacing the components when necessary.

Digital currency interface applications enable the service layers to communicate with the digital currency system. In Phase-1 studies, each operator has its own Service Layer, digital currency interface and a node running on a distributed ledger. Requests are recorded after passing through these system parts in sequence. In the event that relevant changes are made to the configurations of the digital currency interface, it is possible for operators to access other operators' nodes even if their access to their own node in the digital currency system is cut off.

Data interface applications in the Abstraction Layer listen for events in the digital currency system, and feed the results into the data analytics environment. Analytical data can be used to improve the system design, build decision support systems, detect anomalies and make forecasts. On the other hand, operational data includes instantaneous data about the state of the digital currency system. Infrastructure interface applications are tasked with transferring the operational data they obtain by listening to the digital currency system to the Monitoring and Administration Environments. In this way, operational data is used to obtain information about the system and updates can be made quickly when necessary. The participants using operational data and analytical data may be different. For this reason, the layer makes it possible to transfer data to different places.

3.4 Service Layer

Service Layers are financial intermediaries' own regions. Although the financial intermediaries that will provide users with access to digital currency do not need to be operators at the same time, the two roles were handled together in Phase-1 studies and the roles of the intermediaries were assumed by the operators.

The orchestrator applications, agent applications and Application Programming Interface Gateway that financial intermediaries use to connect to core systems are located in this layer. The Service Layer is a logical component rather than a singular physical network. Financial intermediaries' own internal information that is not contained in the distributed ledger can also be stored in this layer. For example, while transactions of users are stored in the digital currency system, the know-your-customer information is only available in the financial intermediary. In addition to the Service Layer, the know-your-customer information can also be stored in different and local systems owned by the financial intermediary.

The financial intermediary gives the user a VC so that the user can access the system. The VPs of requests sent to the digital currency system are checked in the Service Layer, preventing access of unauthorized users to the digital currency system. The Service Layer does not have direct access to the digital currency system. Requests arrive in the digital currency interface in the Abstraction Layer. Orchestrator applications are the first component to which requests that an end user makes via the wallet application are transmitted. Transaction requests from users are transmitted to the digital currency interface via orchestrator applications. If the digital currency interface responds with a confirmation that the transaction was successful, a notification message is sent to the wallet applications using the push notification service. In Phase-1 studies, capabilities such as request routing, load balancing and rate-limiting were also used in the Service Layer.

Unlike other parts of the Digital Turkish Lira System, the Service Layer is designed to allow intermediaries to have different components, services and gateways. The Service Layer can be used together with other systems where intermediaries are involved. The intermediary will be able to migrate its services and some of its business logic to this layer, and offer different services for end users than other intermediaries. For example, the intermediary may offer a conditional payment service that is not available from other intermediaries, or provide a service to store user keys in a secure environment if preferred by users. The services provided are expected to influence end users' choice of intermediary.

In Phase-1, end user access to the Digital Turkish Lira System is provided only through participants with financial intermediary role. However, **in the following phases, service providers not included in the system will be able to provide access for end users by interacting with the system through a financial intermediary.**

3.5 Wallet Application

The wallet application[12] is the end user's access point to the system. Through the mobile application, the user can transfer funds, make payments, request funds, query transaction history and view owned VCs.

In online payments, while ownership of the money can be proved through the wallet application, the money and ownership information are stored in the digital currency system. In offline payments, the money itself will be available on user-managed wallet devices. It is also possible to have flows where payments are made online while the credentials are accessed offline.

Account Identifier

A user of the digital currency system must first have a DID value that identifies them. The DID value can be considered as an identifier that distinguishes the user from others. In order to generate the DID value and the associated key pair, store the key pair, communicate with other users of the digital currency system and store the data used in this communication, a DID agent has been added to the wallet application. A DID agent consists of a key management service, a messaging service, a ledger interface, and a management service that controls these components.

In transfer and payment transactions, money can be sent to the DID value of the counterparty or to the alias assigned to the DID value. At the same time, these transactions can also be executed with a QR code. The QR codes used in the system have been designed in compliance with the TR QR code standard.[13]

Key Management

The key pair consists of a private and a public key. The private key is used to prove the authorization for the created account. Therefore, the private key should be handled in such a way that it is not shared with anyone. The public key is used to verify that the data comes from the relevant user. The key pair is generated by the key management service that is one of the DID agent components on the user's device. The VCs owned by the user are also stored by the key management service.

[12] By technical definition, a wallet is not a structure where money is stored. Wallets are structures that contain cryptographic key pairs and use these pairs to prove ownership in a system. The component called "wallet application" within the scope of Phase-1 is the whole of the mobile application, wallet, DID agent, and local database components.

[13] Regulation on the Generation and the Use of the TR QR Code in Payment Services: https://www.tcmb.gov.tr/wps/wcm/connect/a3dd886f-ac9b-4e1e-b225-58821ccea36e/Regulation+on+the+Generation+and+the+Use+Of+TR+QR+Code+in+Payment+Services+with+annex.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-a3dd886f-ac9b-4e1e-b225-58821ccea36e-nC9xqQW

End-to-end Encrypted Connection

DID agents can talk to each other through an end-to-end encrypted connection after exchanging necessary data including keys with the counterparty. The user connects with other users and intermediaries in the digital currency system through the messaging service in the wallet application, while the agents share their public keys with each other, creating an encrypted connection. The DID agent can also connect directly to the digital identity distributed ledger.

Local Database

In addition to the DID agent, the wallet application also includes a local database. While keys, VCs and other data needed by the DID agent are stored in the DID agent, the application-specific encrypted local database stores the application data. The data in the database are encrypted with the local database key in the secure key store. The secure key store is located in the secure element of mobile devices with Android and iOS operating systems. Only the wallet application can access the key in the secure element. The data stored in the user's local database and DID agent can be used for authorization checks or identity verification in digital identity and digital currency systems.

4. Findings and Assessments

4. Findings and Assessments

Findings obtained during the conduct of the project include multifaceted assessments, and can be grouped under headings such as *Privacy, Financial System, Technology* and *Digital Identity.*

4.1 Privacy

- Cryptographic solutions are employed in the systems to enhance data privacy. However, to provide a more reliable solution compared to using cryptographic solutions alone, segregation of visibility in the entire design is ensured so that no individual actor can access all the information or make sense of it alone.

- No real person information is stored in the digital currency system. It is not possible to link behavioral data with the real persons by examining the account identifiers and account activities of end users. However, the financial intermediary that registers the user in the system is able to establish the link between the natural person and the DID value, which is the account identifier in the current design.

- Thanks to the self-sovereign identity structure, information sharing is kept to a minimum, which will bring about enhanced data security for users.

- If the DID value is shared with many recipients over time, there is a risk that the DID value may be associated with personal information and consumption habits. In this context, to address potential privacy concerns arising from DID sharing in transfers and payments, allowing users to have virtual account identifiers linked to the main account is being considered. A potential design process of the virtual account identifier will be carried out in accordance with the legal framework.

4.2 Financial System

- A banknote is practical, unmediated, unnotarized, plain, final and simple. A digital form of money will not only be a means of payment, but also a **digital version of the banknote.** It will be put into circulation on demand, not to compete with the other forms of money, but to complement them. Accordingly, overcoming the spatial limitations of the banknote will be the key gain here.

- The banknote provides instant finality of transfers and payments. Payment instruments, on the other hand, do not provide instant finality as they require the confirmation of the relevant payment instrument provider, unless their finality is specified by law. In fact, clearing processes are carried out by the relevant payment system operator whose services are utilized by the parties to the payment. This is the main difference between money and payment instruments. Money is instantly transformed into goods and services. Payment instruments, on the other hand, can be transformed into goods and services to the extend that the preferences of the service provider permits. However, some special cases will fundamentally affect user preferences. For example, payment instruments may be demanded more than money due to features such as blocking and refunds. These features are possible because with such payment instruments, transactions are not instantly finalized. On the other hand, cash may be preferred due to the various fees charged by payment instruments and intermediaries. In this respect, **digital currency will not compete with existing payment alternatives and products but can be positioned as an alternative service offered on demand, complementing the payments infrastructure.** What matters here will be the efficiency and integrity of payments, i.e. their capability of having a simultaneous and seamless operation. The digitalization and interoperability of the cheapest, most inclusive and most practical payment types will increase integrated gains for everyone. In this respect, the payment method that enhances the highest capacity in user experience may be more likely to become dominant over time.

- **It is expected that citizens under the age of 18 or that do not have any deposit or payment account for any reason, may prefer digital currency for their payments.** In addition, digital currency will be offered to non-residents, tourists in particular. Improvements are to be made to incorporate practical gains that will facilitate daily life for both groups.

- To meet legal requirements, users could be authorized to use multiple accounts.

- In the case where a user can have separate digital currency accounts on different financial intermediaries, similar to existing bank deposits, the money in the account exclusive to an intermediary becomes inaccessible if there is a service interruption at the financial intermediary. This is contrary to the principle of no dependency on the financial intermediary for the use of the money.

- The Service Layer is designed as the part through which financial intermediaries can participate in the system and value-added products can be included. Creating **areas where the private sector can innovate** will contribute to the development of the Digital Turkish Lira System.

- With the spread of digitalization, assets and things will become more liquid.

- With its **capacity for financial inclusion** in payments and investments, digital currency can make a significant contribution to ensuring equal opportunities in access to both national and global finance.

- **As data will gradually become more open** following the holistic gains in the open economy, open financial services production and open banking, prevention of the monopolization of data will be more possible. Transparent and accessible data -in compliance with the Law on the Protection of Personal Data- will help increase the ability of financial technology firms to access data, which is critical to the development of new products and ensuring competition. Transparency and openness of data will facilitate the removal of barriers to innovations in technical and practical processes.

- It is possible to meet national and international obligations concerning anti-money laundering and combating the financing of terrorism through intermediary institutions and with relevant authorities in charge, similar to the existing flows in financial systems. Anomalies and fraud can be detected through artificial intelligence and machine learning methods. With cryptology-based solutions, privacy of the data for detection purposes can be safeguarded. **Moreover, the ease in know-your-customer methods can reduce the barriers to access to systems and increase the number of financial transactions. High efficiency in the fulfillment of these legal responsibilities can be targeted through data that increases in both quality and size.**

- In the following phases, as digital institutionalization capacity gradually increases, it will become technically possible to identify goods and services subject to economic activity and to monitor prices instantly. With the decline in the need for surveys, one of the milestones in the transition from probability to certainty, all data will be in processable format, with prices in the lead, and instant and uninterrupted access to data will be facilitated.

- **Digital wallets and prepaid application alternatives can be used to deliver money for social relief and support.** In particular, undeniable gains can be achieved in the fight against natural disasters. Delivery of such support will also pave the way for value-added services with very high practical gains.

- The digital Turkish lira is expected to **reduce the overall costs of banknote issuance and operations of currency in circulation.** It is possible to evaluate the differences between physical and digital costs as efficiency gains.

4.3 Technology

- Platformization of systems can widen the participation base in payments and increase ecosystem competencies with all stakeholders. In this context, a platform should be defined not only as a technological component, but also as a social structure that enables new connections between actors and fosters collaborative environments that can be built upon with a participatory approach. The platform approach can serve to establish standards and create an organic ecosystem by ensuring interoperability between components.

- Thanks to the modular structure of the system, each component is easily replaceable. Thus, possible changes impose a minimal impact on other components. Modularity also ensures easier system maintenance and faster adaptation to innovations.

- DLT offers a viable solution against single points of failure.

- With DLT, data templates and communication processes for operators and competent authorities can be standardized. Therefore, processes among institutions can be carried out more quickly and cost effectively.

- In addition to increasing transparency, using a distributed ledger can significantly reduce compliance costs for financial intermediaries.

- **Account-based access refers to the ownership scheme, not to the data structure in the systems.** The relevant data structure can be token-based or balance-based, and both data structures can be used with account-based access.

- **The use of DLT does not mean that the model is decentralized.** While the digital currency system provides decentralization of data and applications within itself, it provides a centralized service to other systems. With operator and intermediary independence, the use of the digital currency system can also become distributed.

- In order for a transaction to be recorded on the distributed ledger, it must be approved by a certain number of node operators according to agreed rules. As the transaction is transmitted to all nodes and this transmission involves cryptographic operations such as encryption or signing, **settlement in distributed ledgers is not as fast as it is in centralized systems.** Therefore, the Transactions Per Second (TPS) of the system is not as high as the TPS capacity of the existing payment systems.

- Distributed ledger technologies in their current form appear to be unable to provide the transaction capacity required for the nationwide rollout of the digital Turkish lira. While it is possible for distributed ledger technologies to provide higher performance through **different designs, software-level modifications and hardware accelerators,** such changes may have consequences such as increased maintenance costs, difficulties in merging with new versions and loss of design flexibility. In this context, it is also considered that new technologies can be designed as **hybrid systems** with existing payment systems technologies, while smart contract features can be handled in separate layers.

- Being employed as an identifier in the SSI model, DID can also be used to identify assets and things as well as natural and legal persons. It is expected to facilitate integration with advanced technology environments such as the Internet of Things (IoT), smart cities and Industry 4.0.

- **Considering the potential gains of identification processes, creating digital representatives of the values in the physical world seems possible.** When the necessary infrastructure is provided, digital asset systems that can be used in conjunction with digital currency and identification systems can be created.

- It is possible and likely for digital ecosystems to be built as a structure where many systems work together. The interoperability of networks is widely studied all over the world. Digital currency systems that integrate distributed ledger technologies into at least one layer are expected to develop in a more concerted way with digital identity and digital asset systems.

- Programmability can be built into money itself, digitized as a token, or it can be implemented for payments at the smart contract and wallet levels. The programmability feature and conditions to be included in money may contradict its role as money because they will limit the use and transformability of money. **In this context, it is thought that the correct concept is not programmable money, but programmable payments.** It would still be possible to design digital tokens that are targeted, time-dependent and convertible into money after use. Whether these digital tokens can be classified as digital currency offered by central banks will depend on their multi-use capacity.

- While it is possible to meet programmability needs with existing payment systems, the dependence of the added programmability capabilities on a single operator of the system may cause a bottleneck. In this case, there will be only limited room for rapid development and innovation. While it is always possible for different actors at different layers to develop their own programmability solutions, it is also possible that new solutions will not be sufficiently widespread and that a fragmented structure will lead to higher compliance and maintenance costs across the entire financial system. **The use of distributed ledger technologies is expected to facilitate the validation, delivery and hosting of programmable payment software.**

- Standards are of great significance for communication among parties. Easing of global communication with digitalization has created the need for compliance with domestic and international standards for the private sector and governments. Many central banks around the world are conducting digital currency research and establishing their own standards. With the Digital Turkish Lira Project, the CBRT is working on its own national standards in case digital currency systems become more common in the near future. The establishment of national standards aims to facilitate domestic processes in the first phase and international processes in the upcoming periods. Currently, digital currency and digital identity operate in the same wallet application created under the project, but **in the following phases,** it is expected that **digital currency transactions will be included in the mobile applications of intermediaries,** while identity wallet transactions will be shaped according to Digital Türkiye[14] services.

[14] https://cbddo.gov.tr/en/digital-turkey

4.4 Digital Identity

- Although SSI is a new and emerging digital identity model, it is considered a promising approach. The ability of individuals to store and control their own data can be an important measure against cybercrimes such as digital identity theft, which is common on the internet; however, legislative alignment of the SSI model is important before it is fully deployed.

- With the SSI model, users can share their information only with the people they want to share it with. **The recipient party can verify the sender, but cannot tamper with the data or access any data other than those shared with them.**

- In terms of use cases and benefits, the SSI model can be used today for passwordless authentication, partial and portable information sharing and know-your-customer processes. In other models, keeping personal information in many different systems can lead to high cost, inefficiency, and problems of expanding the attack surface. With SSI, these burdens can be reduced by only verifying the VP instead of requiring different actors to record new data.

- VCs and their associated keys can be used to authorize payments. Several VCs, including those for financial transactions, can be stored together within the same wallet application.

- It was observed that most of the conditions for programmable payments were related to VCs. Although this implies the integration of digital identity and digital currency systems, they do not necessarily communicate directly with each other. Currently, they communicate through the Service Layer. Although there are multiple Service Layers in the system and scalable implementations within the layer, the feasibility of direct communication between identity and currency systems will also be explored.

- **The know-your-customer VCs obtained through the financial intermediaries that users prefer to register in the system will be retained by the users and can be used for transactions through different intermediaries.** In line with the SSI model, other verifying actors (intermediary institutions) will be able to verify the VPs without being dependent on the identity provider (the intermediary institution performing the know-your-customer process).

- The SSI approach as an identity management model has real-life use in many areas. Still, **it cannot be claimed yet** that the model has made the leap from *early adopters* to *early majority,* within the scope of diffusion of innovations, and **that the SSI approach is used widely.** Nevertheless, it seems possible to move forward by integrating with existing identity solutions. In integration designs, along with hybrid solutions with today's digital identity models, prioritizing standardization efforts can provide significant gains.

- Regarding digital identity integration methods, the diversity of existing identity models can lead to cross-country integrations being built on the assumption that this diversity will continue. Although middleware gateways provide a solution in this context, the lack of scalable solutions brings with it an adaptation cost for each integration. The implementations of SSI models may differ according to jurisdictions, nevertheless, it will be possible to achieve interoperability through standards in the future. In the event that identity schema definitions are universally accepted and standardized, the issue of interconnection between different systems can be reduced from model conversion to platform integration. Portable know-your-customer data is also considered among the data that are in the scope of interoperability. However, there are alternative communication protocols in different implementations of SSI, in this sense, interoperability issues are yet to be solved.

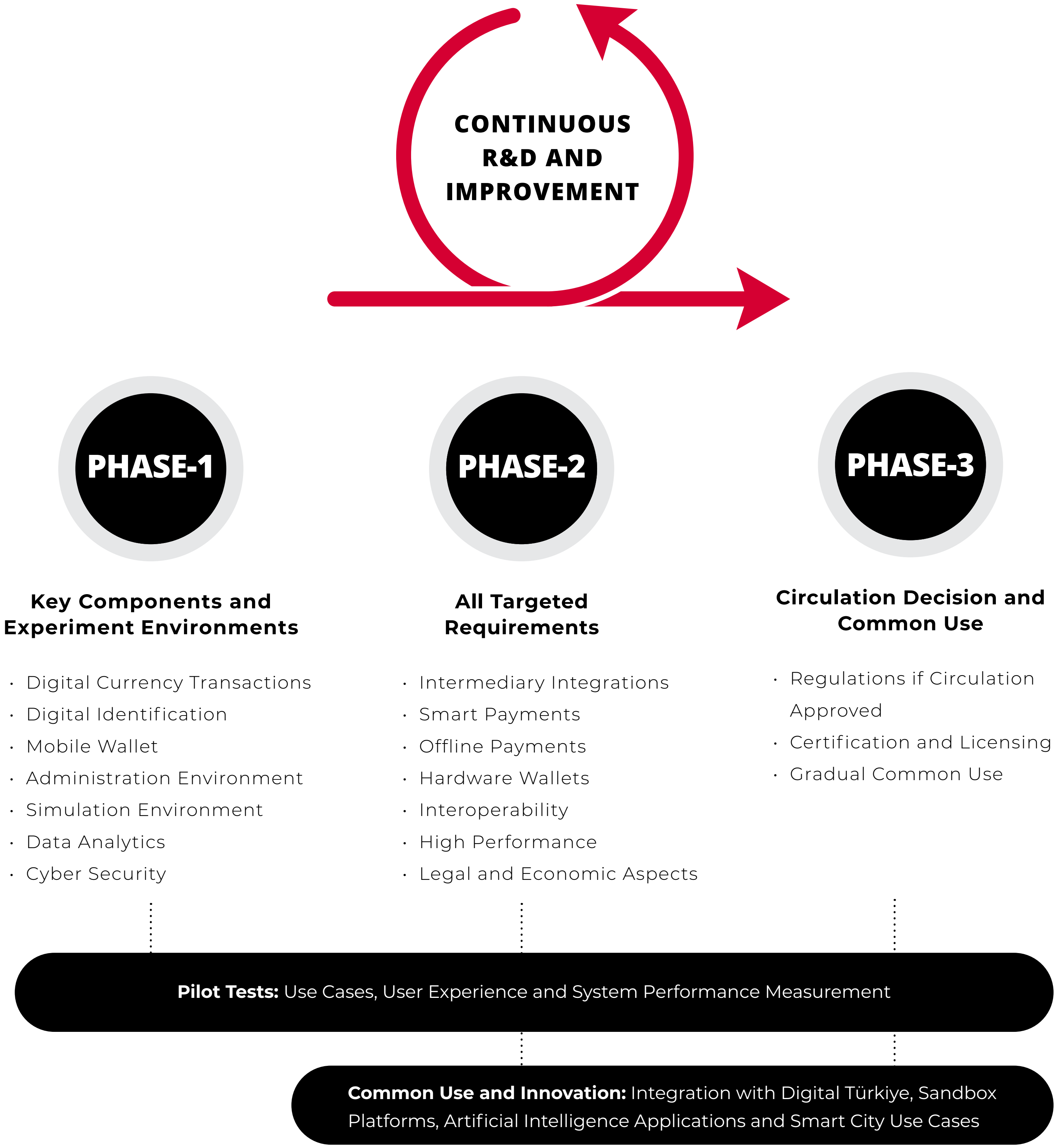
- **Identity and money are digitalizing together.** While digital identity processes occupy the agenda intensively because they are more straightforward, broader and inclusive identification processes are still being explored. The achievements of the pioneers in this area are unique and have the potential to set the standards in digitalization processes.

5. Following Phases

5. Following Phases

> ***R&D activities will continue through following phases. Conversions between forms of the Turkish lira, smart payments, offline payments as well as legal and economic dimensions are among the topics to be addressed in the following phases.***

Apart from the studies carried out with the Platform participants, the CBRT's R&D activities included research, development and testing on interoperability across different networks and technologies, a wholesale payments system on a distributed ledger platform, applications that safeguard data privacy, high-performance architecture designs, comparisons among programmable payment methods, and innovative usage areas.
As for the R&D activities with the Platform participants in Phase-1, studies were carried out on digital currency transactions, digital identification and mobile wallets; experiment environments were prepared; and cyber security operations and data analytics were conducted as elements related to all topics. R&D activities will continue in the following phases, and many topics to be addressed have already been identified. These include **conversions between forms of the Turkish lira, smart payments, offline payments, and legal and economic dimensions.** The planned scope and duration of the phases may vary depending on the results of the studies and evaluations.



CONTINUOUS R&D AND IMPROVEMENT

PHASE-1

Key Components and Experiment Environments

- Digital Currency Transactions
- Digital Identification
- Mobile Wallet
- Administration Environment
- Simulation Environment
- Data Analytics
- Cyber Security

PHASE-2

All Targeted Requirements

- Intermediary Integrations
- Smart Payments
- Offline Payments
- Hardware Wallets
- Interoperability
- High Performance
- Legal and Economic Aspects

PHASE-3

Circulation Decision and Common Use

- Regulations if Circulation Approved
- Certification and Licensing
- Gradual Common Use

Pilot Tests: Use Cases, User Experience and System Performance Measurement

Common Use and Innovation: Integration with Digital Türkiye, Sandbox Platforms, Artificial Intelligence Applications and Smart City Use Cases

The architecture and design of the digital Turkish lira is yet to be finalized. Assessments of the implications of possible design options and whether these options meet the economic, legal and fiscal requirements for the digital Turkish lira are ongoing. Following the assessments, a decision will be made on its circulation.

5.1 Conversions Between the Forms of the Turkish Lira

Conversions between all forms of the Turkish lira will be possible. In the current financial system, deposits in banks can be converted into cash through ATMs or branches. Similarly, **deposits can be converted into digital Turkish lira and digital Turkish lira can be converted into deposits.** This conversion will be possible instantly and continuously. To enable conversions, the digital currency system will be integrated with mobile applications, ATMs, and systems that maintain deposits. For businesses without digital Turkish lira accounts, payments received in digital Turkish lira will be automatically converted into deposits. In these processes, while existing technological opportunities will be further utilized in the most practical way, compliance with the potential innovations in the short, medium and long term will be carefully considered.

In the design of the digital Turkish lira conversion, the Digital Turkish Lira System will be linked to existing mechanisms through which payment service providers manage their liquidity. The Digital Turkish Lira System contains the accounts of payment service providers, the CBRT and end users. To transfer their liquidity to the Digital Turkish Lira System, payment service providers will transfer the amount they want to transfer to the CBRT's account in the system where their liquidity is held. The CBRT will simultaneously issue[15] digital Turkish lira in the Digital Turkish Lira System that corresponds to this amount and transfer it to the account of the relevant financial intermediary institution. If the financial intermediary institution wants to transfer money from the Digital Turkish Lira System to the existing mechanisms, the flow will be reversed.

End users will be able to convert their deposits into digital Turkish lira through the interconnection of these two systems. If end users want to convert their deposits into digital Turkish lira, they will send their request to the financial intermediary institution where the deposit is held, and the relevant financial intermediary institution will transfer digital Turkish lira from its account in the Digital Turkish Lira System to the accounts of the requesting users. At the same time, the financial intermediary will update the balance of the relevant user in its system. If the end user wants to convert the digital Turkish lira into deposits, the flow will be reversed.

From a technical point of view, there are scenarios and integrations already in place for the digital currency conversion processes, and the most efficient approach will be adopted by using the components available at the CBRT. In this regard, a proof-of-concept study has been conducted for a conversion scenario that integrates a bridge application to the CBRT Payment Systems, but a final decision is yet to be made on the method to be launched.

[15] If the technological capacity is sufficient to enable instant supply and distribution of digital currency in response to demand, the need to maintain central bank banknote stocks which is a logistical necessity in banknote management, will diminish over time for the digital Turkish lira.

INTEGRATION WITH DIGITAL ASSETS

The main purpose of money transfers is to make payments in return for goods or services. In the case of goods, a trade transaction can be described as the delivery of an asset versus payment. While the digital currency infrastructure is designed as a new system to realize the payment pillar of a trade transaction, it should be harmonized with the digital transformation in asset transfers, which is the other pillar of the transaction.

In the digital currency system created in Phase-1, transactions take place on a distributed ledger technology network. Similarly, it should be taken into account that the assets themselves or their digital representations may also be exchanged on a distributed ledger technology network, which may be built on a different platform than the distributed ledger platform used in the digital currency system. In this context, with the proof-of-concept study conducted at the CBRT, **digital currency and digital asset networks were created on two different distributed ledger platforms.** The application that has been developed showed that trade transactions operate in a concerted way on these two networks. **Transaction integrity** is ensured in the system. When the trade transaction is completed successfully, the asset is transferred to the buyer and the money is transferred to the seller. In case of unsuccessful completion of the transaction, both the asset and the amount of money subject to the trade remain with their previous owners prior to the transactions.

In line with the proof-of-concept study, it has been found that the digital currency system can be integrated into the distributed asset systems that are likely to be included in our lives in the future, but the methods of integration can create new dependencies.

5.2 Smart Payments

Smart payments, which can facilitate and accelerate payment transactions, are ultimately expected to enhance the user experience. The main types of smart payments are as follows:

Conditional Payments: This is a form of payment in which the amount, the recipient and time of the transfer can be set according to predetermined conditions. These conditions cannot be changed during the process. This type of payment can be used for aid and support money and as conditions set by businesses in exchange for products or services, and is not considered in the scope of the general use of digital currency.

Delivery versus Payment: This is a method of payment that guarantees the delivery of an asset only when and if the movement of money and transfer of funds is completed. It has also been referred to as “atomic” settlement. The scope of delivery versus payment scenarios will further widen with the expansion of the digital asset ecosystem. In addition to the tokenization of securities, digitalization in transfer of ownership that are carried out in physical environment also fall in this scope.

IoT Payments: This refers to the ability of things to make retail payments and, depending on the situation, micro-payments to each other. Payments can be initiated by end users, or they can be carried out automatically between things based on the user’s predefined permission.

Invisible Payments: This is a type of payment that occurs automatically, without interacting with the user, in the background of the event that gave rise to the payment. Despite being a fast-growing field, there are still uncertainties regarding the use of biometric data and the protection of personal data. Once the identification methods to be applied, including thing and contract identities, are clear, it is likely that interconnected payments and automatic accounting can be achieved.

Streaming Payments: This is a payment transaction that occurs continuously while the service is in progress. Instead of making payments before or after the service, multiple payments are made at a certain frequency over a certain period of time.

Definitions and Abbreviations
1 Introduction
2 Central Bank Digital Currency Requirements, Principles and Approaches
3 Digital Turkish Lira Design
4 Findings and Assessments
5 Following Phases
5.1 Conversions Between the Forms of the Turkish Lira
5.2 Smart Payments
5.3 Offline Payments
5.4 Legal and Economic Dimensions
6 Conclusion
APPENDIX

5.3 Offline Payments

One of the most important features of cash is that it allows offline instant payments and transfers. In conventional payments, payments and transfers can be made instantly and irrevocably without the need for an online environment. Similarly, the digital Turkish lira will need to have offline payment and money transfer features in the future. This will support the use of the digital Turkish lira in areas outside the coverage of mobile networks such as rural areas, or in potential disaster areas.

Offline payment is defined in different ways in digital currency projects. **A fully offline payment flow involves the transfer of money between the sender and recipient with no internet connection, and the ability to re-transfer the money received without going online.**

In a scenario where only the recipient has internet connection, the verification process can be carried out online and there is no need to use an offline balance in the online system for the recipient. Therefore, using the offline balance information for the sender will suffice. As spending is made from the offline balance, the sender's offline balance will be updated in the system as the recipient has internet access at the time of payment. On the other hand, **in a scenario where only the sender has internet connection,** the transfer to the recipient takes place without the need for offline balance management for the sender as the sender is online, and only the offline balance for the recipient will be updated in the online system. When the recipient has internet access, it will be possible to add the offline balance to the online balance. In both scenarios, where either of the parties is offline, there are no threats such as double-spending or replay attacks in offline payment.

On the other hand, in a scenario where neither party has internet access, the recipient should be able to perform verification without going online, and the sender should not be able to repeat this process to another recipient who has no internet access. Moreover, the recipient should be able to act as a sender in another flow. If these conditions are fulfilled, the resulting sequence of offline payments across multiple users should be secure, user-friendly and non-privacy invasive.

The basic requirements and design principles also include new requirements with respect to offline payments that need to be taken into account:

- **Security:** The system must be resistant to double-spending or forging attacks. If secure hardware (smart card or device) is used, the hardware must be resistant to tampering.

- **User Experience:** The offline balance stored in a mobile device or another secure hardware should be available in a simple flow and in a reasonable time.

- **Privacy:** If the sequence of offline money transfers is saved, recipients or unauthorized parties should not have access to other users' personal data and account information. While not recording the sequence is an option, there may be benefits of recording so as to detect potential errors in the system. In this case, it is important that the sequence is saved in a way that does not violate privacy.

Another important design choice for offline payments is the medium in which the transfer will take place. In addition to the existing wallet application on smartphones, it may be preferable to use hardware wallets or smart cards that support some form of wireless communication protocol (NFC, Bluetooth, etc.).

- **Smartphone:** In order to develop smartphone applications, the device must have secure hardware that is resistant to tampering. It is possible to develop an application that can store and update balance information and verify an incoming payment in a tamper resistant hardware. However, phone manufacturers develop applications in the secure elements of the devices exclusively in-house.

- **Smart Cards:** It is possible to enable offline payment flows via integrated circuit smart cards with a specific security standard and a tamper-resistant secure area to store data. However, in order to transfer digital currency between the two cards, a third device is required with which the cards will communicate.

- **Hardware Wallet:** From an online account managed via a computer or mobile device, money can be deposited in a hardware wallet using a wired or wireless communication protocol. Money transfers can be carried out by transferring the amount from a hardware wallet to another hardware wallet via wireless communication protocol. Here, the main requirements are to have a secure element in the hardware wallet that is tamper-resistant and to use a secure messaging protocol.

For offline payments, the way information is stored and transmitted is as important as the medium in which it is stored and transmitted. In this context, the design of the cryptographic architecture is the most fundamental and important pillar of the offline payment scenario. The algorithms to be used directly affect security, user experience (time on task and ease of use) and privacy. The main focus of the studies will be on cryptographic algorithms.

Offline payment capacities, which are expected to be especially beneficial in overcoming the difficulties that may arise due to natural disasters and the course of climate change, have already been put on the agenda as a priority issue. The gains to be achieved in this area are also expected to contribute to the formation of digital human capital.

LEGAL REQUIREMENTS

Science and technology-based innovations in the financial sector offer central banks new instruments to carry out their core functions in money issuance and payment systems. Digital currency emerges as **a digital representation of the sovereign currency** as a result of a public need and technology enabling it.

As is the case in all social changes, technological developments have an impact on society and the legal order. Just as the law follows technological changes and can be reshaped according to its effects, the implementation of technological innovation must also adapt to the legal order formed by the needs of the state and society.

During the design process of the Digital Turkish Lira System, the issues required by the **mandatory provisions in our current legislation are also considered,** and the legal arrangements in our current legislation, especially in the Law on the Central Bank of the Republic of Türkiye No. 1211, will need to be followed in the circulation of the digital Turkish lira.

5.4 Legal and Economic Dimensions

In addition to the technological decisions and preferences in the processes for the introduction of the digital Turkish lira, it is also important to examine its legal and economic dimensions. Some of the questions that are still being studied and that may be of interest to potential participants of the Digital Turkish Lira System are given below.

Legal Dimension

- Does the digital Turkish lira need an additional definition?
- Which amendments to the CBRT Law are required for the digital Turkish lira?
- Which legal amendments are required beyond the CBRT Law regarding the digital Turkish lira?
- How will the legislation on personal data protection be implemented in the Digital Turkish Lira System?
- How will the anti-money laundering and combating the financing of terrorism processes be implemented in the context of digital Turkish lira?
- Will any additional legal arrangements be needed for the interoperability of the digital Turkish lira with existing payment systems and cross-border transactions?
- Is there a need for ownership restrictions on digital Turkish lira accounts/wallets?

Economic Dimension

- Does the digital Turkish lira need to accrue interest?
- How will the introduction of the digital Turkish lira affect bank deposits and the existing monetary transmission mechanism? Can transaction and wallet limits restrain a possible shift from bank deposits to the digital Turkish lira?
- How will the digital Turkish lira contribute to economic growth?
- Will the digital Turkish lira improve existing payment systems? What is the optimal framework for integration?
- To what extent will the introduction of the digital Turkish lira positively affect the cost of cash use and banknote management?
- Can the digital Turkish lira make taxation and tax collection more efficient?

In the scope of Phase-1, preliminary work is underway at the CBRT to address these questions, and the findings and answers evaluated together with the designs will be confirmed and concrete implementations will be carried out in the following phases.

WHOLESALE PAYMENTS AND CROSS-BORDER PAYMENTS

R&D studies have been carried out for the use of digital currency in **wholesale payments** independent of the Phase-1 process. The studies carried out for a wholesale payments system, which operates on a distributed ledger platform, protects data privacy and uses gridlock solutions, are aimed to be enriched with various use cases in the future. Digital currency projects for wholesale payments generally examine the efficiency gains that the distributed ledger technology can provide. In this context, research is underway on whether there are efficiency gains in terms of facilitating sharing with common data templates and communication processes, reducing transaction completion times, providing alternative gridlock solutions, and introducing innovations in atomic settlement methods with digital assets.

Wholesale and retail payment systems differ in terms of transaction amounts, transaction frequency, and availability to citizens/institutions. Digital currency can be regarded as money for all, irrespective of distinctions such as retail, wholesale or cross-border payments, and payment systems.

Research into the use of digital currency in **cross-border payments** has been carried out at the CBRT. According to preliminary theoretical and practical findings, the use of digital currency in cross-border payments may bring advantages such as the need for fewer intermediaries, lower foreign exchange transfer costs, increased liquidity efficiency, lower transfer costs and reduced transfer times.

For cross-border payments, as opposed to operations involving multiple correspondent banks, more efficient structures can be established with more predictable user fees. Many central banks and international organizations have been widening the scope of their work in this area, as it holds significant potential for the near future.

Within the scope of the project, the field of cross-border payments is still at the research level. It is planned to cooperate with national and international institutions and organizations in the future. The high cost of cross-border payments increases the demand for digitalization, and many interdependent or completely independent projects are being carried out simultaneously around the world. The proof-of-concept and R&D activities targeting interoperability in local ecosystems are expected to contribute to cross-border payments as well.

6. Conclusion

6. Conclusion

The Central Bank Digital Currency has already entered the agenda of many countries as a natural consequence of digitalization. There will likely be a need and a suitable ground for digital currencies to enter circulation in the future. Accordingly, the Central Bank Digital Turkish Lira Research and Development Project has been launched and the first phase of the project has focused on **technological dimensions** by determining the requirements for the use cases and architecture of the digital Turkish lira. In the scope of the technological dimension, the project working environment has been prepared, related systems and applications have been developed and simulations and tests have been carried out. In addition, system performance and user experience have been measured and analyzed through pilot tests.

In line with the principles and approaches defined by the CBRT, the Digital Turkish Lira System is being designed in a way that **protects privacy, does not harm existing economic and financial processes, is able to adapt technological innovations, is interoperable with components in digital ecosystems, and is accessible with no dependence on any financial intermediary institution.** The **modularity** approach aims to avoid dependence on any single technology.

As part of the first phase, a prototype Digital Turkish Lira System was prepared with the participants of the Digital Turkish Lira Collaboration Platform. Digital identities were created for system operators and test participant users in the Digital Turkish Lira System to be used in financial transactions. **Via digital wallets, pilot test users have performed different levels of identity verification, stored their documents and used them in financial transactions.**

Apart from the studies carried out with the platform participants, performance experiments have been conducted for various strategic advanced technologies and comparisons were made with existing instant payment system technologies in-house within the CBRT. **Alternative scenarios for the integration of the Digital Turkish Lira and the CBRT Payment Systems have been evaluated.** Integration applications have been developed for the scenarios identified in the scope of Phase-1 and tests have been completed successfully.

In addition to the technological requirements of the digital Turkish lira, studies are carried out on the **economic and legal** framework. During work on the legal aspects of the digital Turkish lira, it was decided that digital identification was critical for the project, and it was decided to prioritize work in this area. The digital identity system with its technology and standards will be determined in the framework of Digital Türkiye studies. Wallet applications and related digital identity software in intermediary institution systems will be shaped according to country standards. Use of digital identities within the scope of digital currency will also be developed in line with the standards.

The near, medium and long term effects of the digital Turkish lira will vary depending on the architecture and design of the digital currency and the policies to be implemented. The design is intended to be dynamically responsive to needs. In the following phases, work will continue on high performance and interoperability issues to meet the requirements of a digital Turkish lira.

Digitalization offers important gains in terms of innovation capacity. Efficiency gains of the national currency will be maintained in the current production, distribution and management procedures and principles. The digital Turkish lira will be complementary to the existing currency form and the initial aim will be to eliminate the spatial limitations of banknotes. In addition, the digital Turkish lira is intended to be designed and introduced in a way that will serve as the basis for innovations that will be the source of productivity increases in the financial field, with the payments ecosystem being a priority.

Access to digital Turkish lira will be facilitated by licensed financial intermediaries, including commercial banks. In this context, the total amount of cash that can be circulated in digital wallets as well as spending limits will be managed in a gradual and controlled manner, taking into account the **two-tier banking system principles** -one of the pillars of a free market economy- and the **principle of not harming the financial system.** From this point of view, the process is in line with the traditional banking approaches.

In studies worldwide, digital currencies are envisioned to play a **complementary role to cash** in existing systems. The studies on the digital Turkish lira are carried out with a similar design approach. The CBRT will take all technical and administrative measures to ensure that both conventional banknotes and the digital form remain in circulation as fully complementary to each other and to build capacities in line with demand and needs.

The integrated ecosystem for wholesale and retail payments, which is operated in line with the principle of seamless payments as a prerequisite for financial stability, will become more practical, more inclusive and more sustainable with the introduction of the digital Turkish lira.

Many of these gains are the results of designs that can be considered as the intersection of digital currency studies conducted around the world. After the customized designs, effects will be observed in line with the principles and approaches determined by the CBRT. Different designs will bring about different results with respect to establishing digital ecosystems and reaching sufficient utilization.

The development of the digital Turkish lira will be a continuous process. As is the case in any digital product, continuous improvement and absolute security approaches must be adopted and maintained for the digital Turkish lira. With ever-increasing computational power and ever-decreasing technology costs, the strategic technologies available in the digital currency space are expected to change and evolve continuously and multidimensionally in the near, medium and long term. Therefore, the Digital Turkish Lira Project will constantly remain on the research and development agenda.

APPENDIX
Digital Identity Models

Digital identity refers to all the information that represents a natural or legal person and is utilized by these persons to access various services in a digital system. Persons use it to prove their identities or attributes in digital networks. The most prevalent method of identity verification on a service is to create an account with a password using e-mail or mobile phone information. There are historically three leading methods used to manage these accounts.

The simplest method uses the model where each account is stored on the website where it is registered. However, there are some difficulties in sustaining this model due to the formation of identity silos. Given the large number of digital services, using different passwords on each website makes identity management difficult for users. On the other hand, giving the same password to different websites brings with it the potential threat of identity theft. Keeping personal data in a large number of different service providers increases attack surfaces.

The second method, federated identity, enables connection to other websites through a single identity provider instead of registering with each website separately. This allows the user to memorize only a single password and username. Although this method is widely used today, it requires users to trust the identity provider and may create a single point of failure in the system. In fact, under the scenario where all services are accessed with a single provider, if the identity provider cannot be accessed, identity verification will not be possible in any service. In addition to this risk, identity providers become favorite attack points. Another important and potentially disadvantageous aspect of this method is that the personal information of the users is under the control of the identity provider, not the users themselves.

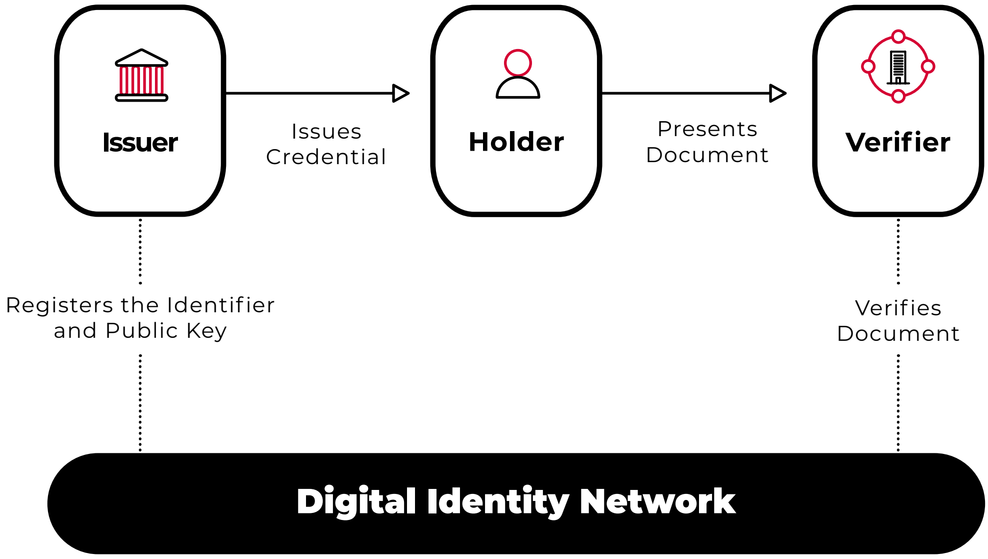
To sum up, the common feature of these two methods is that the **data are stored centrally.**

The third method, Self-Sovereign Identity (SSI), allows users to store their personal information themselves and gives them control over their digital identities. In this approach, individuals can take their identities or related digital credentials from the identity provider and store them on a device or environment that is under their own control. The credential contains the proof that it has been issued by the provider, and the information that allows access to this proof through cryptographic operations. Thus, a person can prove that the credential is their own and that they have received it from a real provider. Once the credential is issued, the provider does not need to store user data. In the SSI model, as in other methods, there are central authorities even if distributed ledger technology is used.

Central authorities determine identity schemas, while identity providers generate Verifiable Credentials (VCs) according to the identity schema and the definitions. However, unlike other methods, in the SSI model, users can perform verification independently from the identity provider. Identities and credentials can be verified over a shared network (usually a distributed ledger) without being dependent on the identity provider and the identity provider's infrastructure.

There are three main actors in the SSI model. The actors and their roles are summarized below:

- **Issuer:** An actor that issues VCs to other participants upon request. As public and private institutions are expected to assume this role, it usually takes place on centralized servers.
- **Holder:** An actor that stores and manages VCs generated for them and can prove their identity and authorization by using these VCs. Since end users, especially individual users, are expected to be in this role, it is usually carried out through wallet applications running on personal devices.
- **Verifier:** An actor that verifies the documents presented by other participants and users by accessing the digital identity network. All users can take on this role.



In the SSI model, when a person wants to prove their identity or a specific characteristic (being over 18 years old, being a university student, etc.), they can share only the portion of information that is enough to verify that they have the requested qualification, without the need to share all the details of their identity. In addition to the importance of protecting personal data, the advantages of the SSI model are becoming even more prominent as the benefits that users can gain from their own data increase day by day.

TÜRKİYE CUMHURİYET
MERKEZ BANKASI